

CRISIS COMMUNICATION PLAN



CRITICAL INCIDENT RESPONSE GROUP

Table of Contents

Crisis Communication Plan

FBI	3
- Executive Bios	3-11
- Critical Incident Response Group	12
Crisis Rating Assessment	13
- Likelihood Impact Map	14
Current Crisis Overview	15
- SWOT Analysis	16
- Crisis Stakeholders	17
Communication Flow Chart	18-19
Crisis Response Guidelines and Checklist	20-22
Crisis Communication Team Members	23-24
CIRG Management Team	25-26
Internal FBI Communications Teams	27
Media Contacts	28
Public Affairs Specialists	29-30
Key Media Outlets	31-32
FBI Fact Sheet	33
Media Strategy	34
- Key Messages	34-35
- Key Audiences	36
- Communication Platforms	37
- Potential Media Questions	38
- Media Do's and Don'ts Guidelines.....	39
- Social Media Plan	40-42
Media Examples	43-51
- Holding Statement	52-54
- Social Media Posts.....	55
- Media Kit	56-59
Templates	
- Incident Report.....	61
- Media Inquiry Log	62
- Evaluation Form.....	63-64
- Media Sign-In Sheet	65
- Key Messages	66
- Social Media Templates.....	67
- Media Advisory	68
- News Release	69

FBI Mission:

To protect the American people and to uphold the Constitution.

This should be highlighted in every public communication statement.

FBI's Vision Statement:

Ahead of the threat through leadership, agility, and Integration.

Executive Bios

Kash Patel

Director



Bio:

During the first Trump Administration, Mr. Patel led President Trump's counterterrorism mission as deputy assistant to the president on the National Security Council, overseeing the elimination of senior al-Qaida and ISIS leadership and the safe repatriation of American hostages. He also served as deputy director of National Intelligence, supervising all 17 IC agencies, and briefing critical intelligence to the president daily. In 2020, he became chief of staff to the Department of Defense, managing over three million employees, a \$740 billion budget, and \$2 trillion in assets.

Dan Bongino

Deputy Director



Bio:

Appointed deputy director of the FBI in February 2025 by Director Kash Patel, Mr. Bongino holds a bachelor's and master's degree from the City University of New York and a master's from Penn State University. He served in the Dignitary Protective Division and the elite Presidential Protective Division during President George W. Bush's administration. He later transitioned to criminal investigative work in the Baltimore Field Office, leading a multimillion-dollar fraud investigation resulting in successful prosecutions.

Andrew Bailey

Co-Deputy Director



Bio:

Appointed co-deputy director of the FBI in September 2025, Mr. Bailey began his legal career as a special prosecutor and assistant prosecuting attorney in Missouri.

He served as general counsel for the Missouri Department of Corrections and Governor Mike Parson, and later as Missouri's 44th attorney general. He won election to a full term as attorney general before joining the FBI leadership team.

Roman Rozhavsky

Assistant Director, FBI Counterintelligence Division



Bio:

Direct all the FBI's counterintelligence operations worldwide and implement the U.S. Government's strategy to defeat hostile foreign intelligence services. As Deputy Director of the National Counterintelligence Task Force in 2019, he helped create a nationwide framework for integrating federal, state, and local efforts against foreign intelligence threats. As Section Chief from 2023 to 2024, he managed all FBI efforts to detect insider threats across the U.S. government — including espionage, mishandling of classified material, and unauthorized media leaks.

Don Holstead**Assistant Director, Counterterrorism Division****Bio:**

Holstead brings over two decades of frontline and leadership experience with the FBI, making him uniquely qualified for one of the agency's most critical national security roles. His appointment comes after serving as Deputy Director of the National Counterterrorism Center (NCTC), where he worked at the strategic center of U.S. counterterrorism efforts across government. Throughout his FBI career, Holstead tackled high-stakes national security threats including those posed by ISIS, al-Qaida, and Iran-backed actors.

Brett Leatherman**Assistant Director, Cyber Division****Bio:**

Brett serves as a senior executive managing the FBI's strategy to impose cost on some of the most sophisticated cyber adversaries targeting US interests. He graduated from Cornerstone University with a degree in Computer Information Systems and received a master's degree in Cybersecurity Risk Management from Georgetown University. Brett holds several widely recognized cyber certifications and speaks domestically and internationally on emerging national security and cyberthreats.

Jason Kaplan

Assistant Director, International Operations Division



Bio:

Kaplan entered on duty as an FBI Special Agent January 2004. From 2004 through 2011, he was assigned to the FBI New York Field Office where he specialized in dismantling transnational gangs. During his tenure in NYO, Mr. Kaplan was a Senior Instructor for the FBI Underwater Search and Evidence Recovery Team (USERT). In July 2024, the Director selected Mr. Kaplan as Deputy Assistant Director of the International Operations Division. In May 2025, Mr. Kaplan was promoted to be the Assistant Director of the International Operations Division overseeing all international offices, employees, and operations.

Timothy A. Ferguson**Assistant Director, Criminal Justice Information Services Division****Bio:**

Led a team of over 3000 personnel in the FBI's largest division, overseeing operations and enhancements of national law enforcement databases accessed and utilized millions of times per day. Managed threat mitigation in the National Threat Operations Center and provided exceptional customer service through firearms background checks.

Steve McQueen
Assistant Director, Threat Screening Center



Bio:

Led and directed FBI Counterterrorism and Counter Proliferation investigations/operations throughout the majority of Pennsylvania and Southern New Jersey to ensure proper case direction, focus and compliance. Directed, managed, and supported special agents, task force officers, and analysts in providing strategic, operational, investigative, and infrastructure support to the Domestic Terrorism Program.

Critical Incident Response Group:

The Critical Incident Response Group for the Federal Bureau of Investigation has been tasked with managing all crisis-related incidents. It enables the FBI to rapidly respond to and effectively manage special crisis incidents in the United States. Their job is to provide rapid assistance during a crisis. Crises that can require, but are not limited to, the help of the Critical Incident Response Group are cases involving the abduction or mysterious disappearance of children, crisis management, hostage negotiation, criminal investigative analysis, and Special Weapons and Tactics.

The Critical Incident Response Group assists in the assessment, selection, and training of FBI undercover employees.

Crisis Definition

A situation that poses a significant threat to the safety of the American people, FBI operations, and reputation, requiring immediate and coordinated attention.

A crisis in terms of the FBI can involve unexpected loss of life, threat to life, privacy of American lives, safety in governmental structures, and much more.

Purpose

Timely and accurate communication with internal and external stakeholders of the FBI is essential in the event of a crisis. While each crisis will require a unique response, this plan can be utilized to issue to inform chiefs, sheriffs, command staff, and public information officers on how to respond in the event of a crisis by utilizing the provided resources below.

Likely Organizational Crisis' / Rating Assessment

Likelihood: the probability or chance that a crisis will occur

Impact: the range of consequences a crisis has on individuals, organizations, etc.

Priority: a system for determining the most critical needs and actions during a crisis

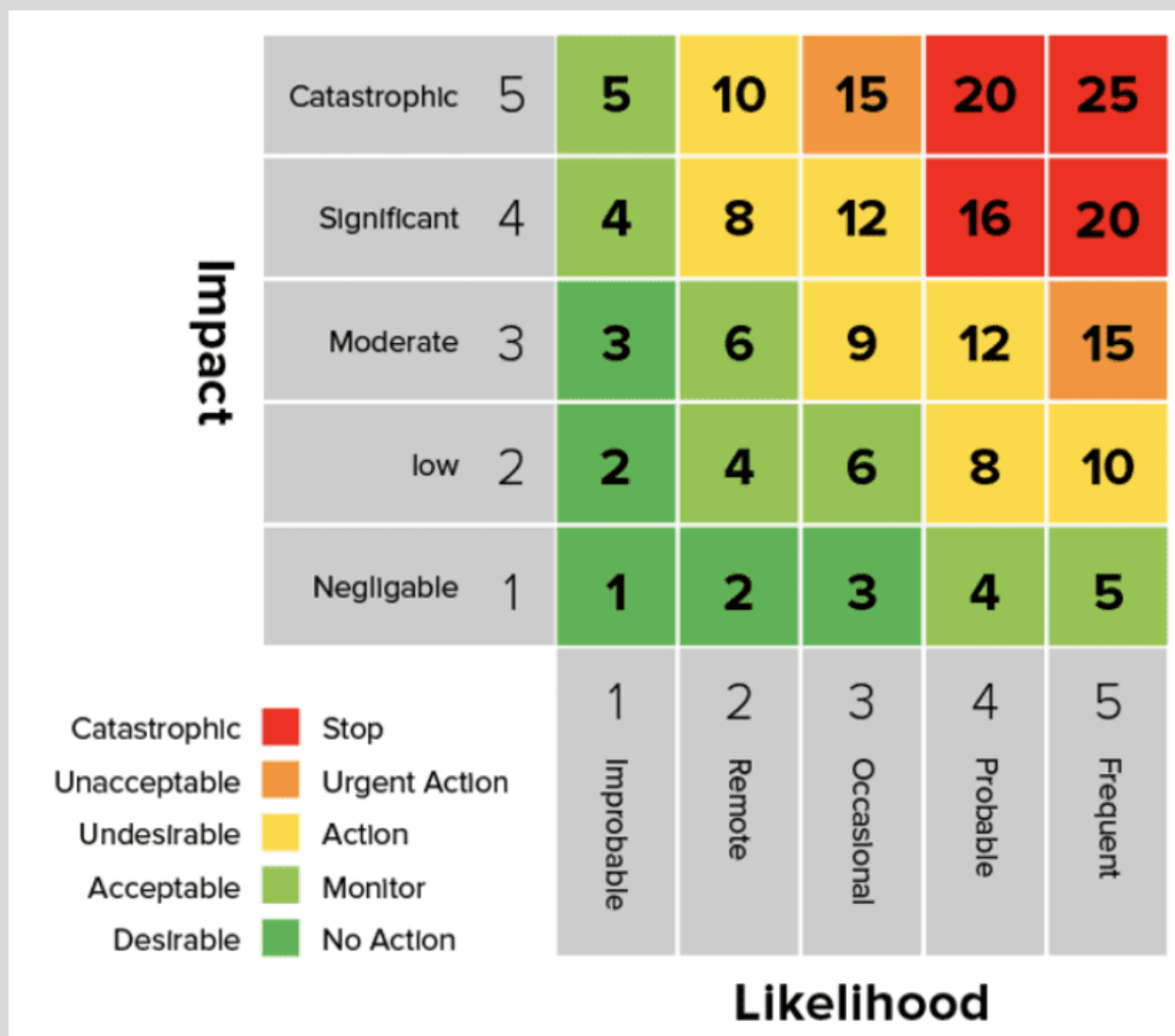
- $\text{Priority} = \text{Likelihood} \times \text{Impact}$

Higher Likelihood & Impact = Higher Priority

1. Terrorism – Violent, criminal acts committed by individuals and/or groups who are inspired by, or associated with, designated foreign terrorist organizations or nations.
 - a. Likelihood: 3 - Occasional
 - b. Impact: 5 - Catastrophic
 - c. Priority: 15
2. Active Shooter Events - One or more individuals engaged in killing or attempting to kill people in a populated area.
 - a. Likelihood: 5 - Frequent
 - b. Impact: 5 - Catastrophic
 - c. Priority: 25
3. Organized Crime – associations of individuals who operate, wholly or in part, by illegal means.
 - a. Likelihood: 4 – Probable
 - b. Impact: 3 - Moderate
 - c. Priority: 12
4. Cyberattacks – malicious cyber activity threatens the public's safety and our national and economic security.
 - a. Likelihood: 5 - Frequent
 - b. Impact: 4 - Significant
 - c. Priority: 20
5. Espionage – the act of secretly obtaining or transmitting information for the benefit of a foreign power, with the intent to harm the U.S. or aid a foreign nation.
 - a. Likelihood: 3 - Occasional
 - b. Impact: 5 - Catastrophic
 - c. Priority: 15
6. Kidnappings / Missing Persons – unlawful seizure and confinement of a person, often involving interstate transport, and may include holding them for ransom.
 - a. Likelihood: 4 - Probable
 - b. Impact: 4 - Significant
 - c. Priority: 16
7. Hostage Situations – seizing or detention of an individual coupled with a threat to kill, injure, or continue to detain such individual.
 - a. Likelihood: 2-Remote

- b. Impact: 5 - Catastrophic
 - c. Priority: 10
- 8. Reputational Crisis - an incident that may cause the public to lose confidence in FBI Leadership
 - a. Likelihood: 4 - Probable
 - b. Impact: 3 - Moderate
 - c. Priority: 12

Likelihood and Impact Heat Map Chart



Current Crisis Overview

The FBI is currently navigating heightened public scrutiny surrounding recent leadership changes, increased interagency collaboration with U.S. Immigration and Customs Enforcement, and the ongoing Jeffrey Epstein investigation. The appointment of FBI Director Kash Patel has created intense media attention; however, the FBI remains committed to showcasing its values of accountability, integrity, and transparency within its leadership. Additionally, the FBI's interagency collaboration with ICE in carrying out federal immigration laws within the U.S. has become a political and emotionally charged issue, drawing questions from the American public surrounding public safety. Finally, the FBI is continuously investigating and confirming evidence surrounding the Jeffrey Epstein case. The FBI continues to face public pressure surrounding the release of evidence, causing the American public to question the transparency and the alleged political sway of prominent figures preventing the release of the files. These three events have caused increased scrutiny of the FBI, and it is essential to address these crises with transparency and clear communication to reinforce public trust.

SWOT Analysis

Strengths	Weaknesses	Opportunities	Threats
1. Established institutional credibility. 2. Effective Cross-functional Collaboration 3. Diverse Teams that lead to fostering cohesive group dynamics 4. Effective Team Communication 5. Highly specialized & Continuously Trained Workforce	1. Leadership appointment controversies Internal strain 2. Communication Gaps 3. FBI had not fully implemented key information security program activities for the critical network reviewed 4. Resistance to technological changes 5. High-stress levels within employees posing challenges to their wellbeing	1. Reinforce public trust. 2. Specialized Team Training Programs 3. Recognition systems and wellness initiatives 4. Room for individual growth, motivation, and overall well-being 5. Leadership Development	1. Internal turmoil or differences 2. Lack of group accountability 3. External factors that impact team dynamics 4. External Threats to internal communications 5. Rapid technological advancements

Crisis Stakeholders

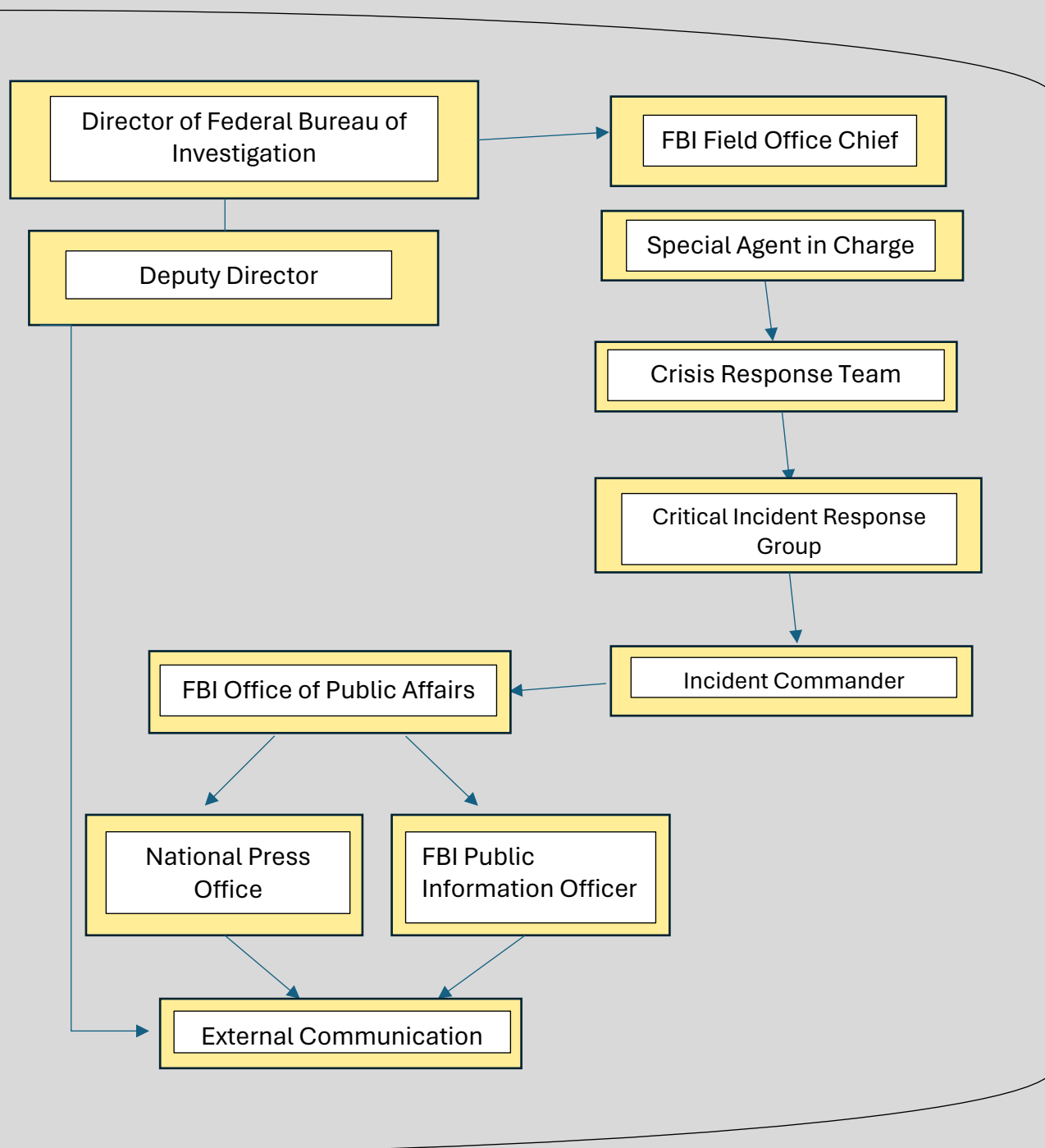
Internal Stakeholders

- FBI Director
- FBI Executive Leadership
 - Chief of Staff
 - Deputy Director
 - Associate Deputy Director
- Office of Public Affairs
- Office of Congressional Affairs
- Office of the General Counsel
- FBI Personnel
- Specified Field Offices
 - Intelligence Branch
 - National Security Branch
 - Criminal, Cyber, Response, and Services Branch
 - Science and Technology Branch
 - Information and Technology Branch
 - Human Resources Branch

External Stakeholders

- General Public***
- Federal Agencies
- Department of Justice
- Congress
- Media
- Victims
- White House
- State Law Enforcement

Communication Flow Chart



Notification to FBI Field Office

FBI Field Office Duty Agent/Special Agent in Charge

- Collects initial facts.
- Confirms credibility.
- Activates internal notification.

Crisis Response Team

- Tactical Group (SWAT)
- Intelligence analysts
- Crisis Negotiation Unit
- Operational Support

Critical Incident Response Group

- validates the scope of the crisis.
- synchronizes messaging with field offices and other external agencies.

****Depending on the crisis, the next step could implement a unified command approach****

- FBI command
- Local/state Law Enforcement
- Other Federal Partners (Secret Service)

Incident Commander/FBI Office of Public Affairs

- Directly speak to the public
- Work to maintain the Public informed during and post-crisis.

National Press Office/FBI Public Information Officer

- Press briefings
- Media statements
- Social media messaging
- Control of rumor or fake news surrounding the crisis

Crisis Response Guidelines & Checklist

In the event of a crisis, the FBI must be prepared for attention from national media, coverage by social media, families, and civilians, whether directly involved or not in the ongoing crisis. A well-thought-out and structured initial response to heightened fear after a crisis is crucial to effective communication.

Pre-Event:

- 1. Maintain an updated contact list for all area Public-Information Officers**
 - Police, Fire, EMS, FBI
 - City Officials, schools, public venues, hospitals, morgues, etc.
 - Names, titles, all phone numbers, and email information
- 2. Pre-identify methods available for joint communications.**
 - Email lists, conference call capabilities at each agency
 - Develop a Memorandum of Understanding with the surrounding public agencies to assist with media response.
 - Obtain proper names and titles for all agency chiefs.
 - Obtain digital seals for each department for press releases.
- 3. Obtain local media contact information, including means to deliver press releases.**

Onset of Crisis

- 1. Request additional media assistance.**
 - Staff will answer phones, manage press conferences, maintain a media log, coordinate with Incident/Unified Command, navigate social media, and write press releases & talking points for officials.
- 2. Determine whether the information can be released within the first minutes by dispatchers in response to calls from other first responders, media, and the public.**
- 3. Coordination among Public Information Officers**
 - Identify and contact PIOs from all entities affected.
 - Agree on the preferred method for joint communication and whether email chain, bridge line, or conference calls.
 - Agree to limit investigative information release to agencies on a need-to-know basis.
 - Identify a single agency and phone numbers to which all media calls will be referred for official information.
 - Identify the agreed-upon re-contact time. Agree with information, if any, that may be released while initial coordination efforts are underway.

Possible occurrences during the onset phase of the crisis:

MAY: release staging area for media trucks, identify agency assets responding to the scene (SWAT, Bomb Squad, etc.), and identify lead agency for media calls

MAY or MAY NOT: confirm certain incident details surrounding the crisis.

MAY NOT: Answer questions regarding other agency responders and indicate numbers or statistics of loss of life or threat to civilian life, dependent on the crisis.

4. Coordinate with Incident/Unified Command

- Identify the PIO who will maintain contact with Incident/United Command
- Identify the incident spokesperson.
- Determine what information can be released immediately to assist the investigation and allay public concern to include:
 - type of incident occurring
 - Agencies responding
 - Location of incident
 - Number of Suspect(s)
 - Cautions and Directions to the Public
 - Whether suspect(s) are at large
 - Road closures, alternative routes
 - Family reunification location
 - Closing or lockdown of schools or other facilities
- Brief Incident/Unified Command on current information in the media
- Identify the initial staging area for media trucks and cameras.
- Identify a potential press conference location.
- Identify what information, if any, police/sheriff department dispatchers and personnel can confirm.
- Relay all information to the group PIOs.

Updating the Media:

- 1. Determine whether a press conference will be held.**
 - Assign a coordinator.
- 2. Determine whether a press statement or press release will be issued.**
 - Assign writer.
 - Obtain sign-offs from all agencies.
- 3. Ensure victim coordinators know what is being released to the press.**
- 4. Maintain a log and document media contact for post-incident needs.**

Pre-press Conference Checklist

- **Identify the speaker(s) and where they will stand, and the speaking order.**
- **Identify a media person to manage the conference.**
- **Coordinate talking points with Unified Command.**

****Talking points must answer questions about who, what, when, where, how, agencies involved, victims, volatility of situation, where involved family members should go for information, and when the next press briefing will occur. ****

- **Ensure talking points convey and recognize the gravity of the event, sensitivity to the victims.**
- **Talking points answer what you cannot provide at this time and why.**
- **Prepare the speaker to respond to rumors and social media reports.**

****Important to ensure DA, SA, or US Attorney is involved as needed in press conference****

Second & Following Press Conference Checklist

- Brief speakers on information currently being reported.
- Focus talking points on the new information available.
- Provide timely information.
- Clarify facts of the case, especially when rumors persist in the media.
- Identify when the next press conference will occur.

Crisis Communication Team Members

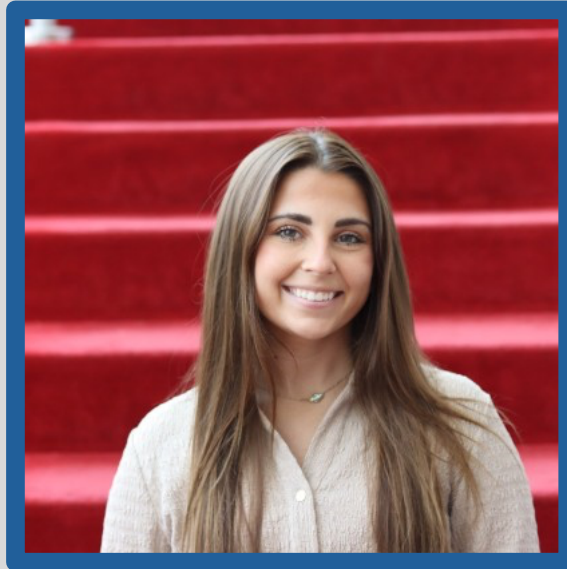
Emmie Cancro
ercancro@unc.edu
919-623-8280



Khloie McClain
Khloiegm@unc.edu
336-558-9928



Raegan Fulghum
raegancf@unc.edu
252-640-7424



Critical Incident Response Group Management Team

Kash Patel
Director of FBI



Paul Haertel
Assistant Director
(703) 632-4101



Robert W. “Wes” Wheeler
FBI Chief Officer in Chicago



Internal FBI Communications Teams

Press Contacts:

FBI National Press Office:

Number: (202) 324-3691

The National Press Office is tasked with releasing official press releases from the Federal Bureau of Investigation about ongoing crises that are of public attention. These press releases come directly from the Bureau and are intended to provide the public with accurate information.

Multimedia Productions Group

Number: (304) 625-5820

The Multimedia Productions Group works closely to utilize new technology to visual life. Recently, they have developed video technology to reenact and describe moments leading up to crisis events.

Office of Public Affairs

The office of Public Affairs is the most important point of contact for the U.S. Department of Justice with the media and news outlets.

The Office is responsible for ensuring that the public is accurately informed about recent crises and the Department of Justice's recent activities. Also is responsible for informing the public about the priorities and policies of the Attorney General and the President in their regard to law enforcement intel and legal affairs regarding crisis.

Office of Public Affairs Direct Line:

(202) 514-2007

Department of Justice Main Switchboard:

(202) 514-2000

Media Contacts

Local Media

NBC 4 Washington	Anthony Mague, News Director	isee@nbcwashington.com	(202)885-4000
WTOP Radio	Julia Ziegler, Director of News and Programming	jziegler@wtop.com	(202)895-5000
WMAR2 News	Kelly Groft, news Director	newsroom@wmar.com	(410)372-2590
WUSA 9	Caridad (Cari) Hernandez, News Director	chernandez@wusa9.com	(202)895-5999

Regional Media

CBS News	Tom Cibrowski, President & Executive Editor	evening@cbsnews.com weekend@cbsnews.com	(212)975-3247
CNN	Adam Cohn, Executive Vice President and Chief Financial Officer for CNN Worldwide	cnn@cnn.com	(301)883-2482.
NPR	Katherine Mahr, President & Chief Executive Officer	https://help.npr.org/contact/s/	(202)513-2000
Fox News	Lachlan K. Murdoch, Executive Chair & Chief Executive Officer	https://help.foxnews.com/hc/en-us/requests/new	(888)369-4762

Public Affairs Specialists

These individuals handle media inquiries, develop new and ongoing media coverage, and act as a liaison between the FBI and the National and local media outlets. Each field office has a designated Public Affairs Specialist, and depending on the area, these specific specialists will assist with directing information from the bureau to the public.

Shelley Lynch

Public Affairs Specialist

Charlotte, NC



Sofia Kettler
Public Affairs Specialist
Philadelphia, PA



E. Wade
Public Affairs Specialist
Washington, District of Columbia



Key Media Outlets for CIRG

Traditional Media:

1. Broadcast Media: Television Broadcasts, Press Conferences, & Radio Guest Appearances

This is the key media outlet used by the FBI in cases of crisis. The Crisis Incident Response Group uses verbal and live broadcast media to accurately express information in times of heightened public fear and imbalance. This verbal and visual use of media is important in cases where there need for immediate reassurance that the FBI is working diligently in a time of heightened crisis.

2. Print Media: Newsletters & Newspapers

This is still important to reach an audience that may not first be reached through broadcast media. The same message is portrayed in written form as was stated in visual form.

Digital Media:

1. Online Newspapers, News Agencies: CBS, NPR, CNN

In the digital age, it is important to maintain physical and online newspaper articles to inform the public. This messaging is the same as the previous two, but in an online format with important news agencies. The messaging is clear and concise, with the mission stated in an obvious manner.

2. Social Media: X, Instagram, YouTube

Maintaining a social media presence in times of crisis is of utmost importance. This is the time when newly updated information should be released to the public in a timely and concise manner, avoiding confusing jargon or emotion.

3. Websites: [fbi.gov](https://www.fbi.gov)

The official website of the FBI (listed below) will also be used to express the same messaging in another format to reach more public audience. This is more credited like other accounts directly administered by the FBI because it is directly coming from this agency. The messaging tactics are the same as before but are used to inform the public about seeking facts of the crisis. Ensuring the public that the crisis is being mitigated is of importance as well.

Owned Media:

1. Social Media Accounts:

Social Media accounts run by official FBI personnel will be viewed with the highest regard in times of crisis. This outlet will be used frequently, especially to inform the public of recent

developments, and will also be used to connect to the public on an emotional level while expressing concern or sympathy in times of crisis.

Earned Media:

1. Press Coverage

This is an important used but can be out of the control of the Critical Incident Response Group when other press outlets cover the crisis. Can times hurt or help the crisis and the public's perception of it, but it is recommended to be prepared for both. Press will cover any incident as it is their right, so take the outcome and focus back to the main message of public safety to the public.

Media outlets and their importance/usage in times of crisis depend on the incident at hand. It is important to know that some coverage of the crisis will not focus on the main message of the Critical Incident Response Group, but it is important to use this to re-guide the public back to the work that is being done to prevent a similar crisis from happening again.

FBI Fact Sheet

- FBI stands for the Federal Bureau of Investigation.
- On July 26, 1908, Attorney General Charles J. Bonaparte appointed an unnamed force of special agents to be the investigative force of the Department of Justice. The FBI evolved from this small group.
- The FBI's mission is to protect the American people and uphold the Constitution of the United States.
- The FBI employs approximately 38,000 people, including special agents and support professionals such as intelligence analysts, language specialists, scientists, and information technology specialists.
- The FBI is headquartered in Washington, D.C. The offices and divisions at FBI Headquarters provide direction and support to 56 field offices in big cities, more than 350 smaller offices known as resident agencies, several specialized field installations, and more than 60 liaison offices in other countries known as legal attachés.
- The FBI is led by a director, who is appointed by the U.S. president and confirmed by the Senate for a term not to exceed 10 years. The current Director is Kash Patel.
- The FBI's investigative authority is the broadest of all federal law enforcement agencies. The FBI has divided its investigations into several programs, such as domestic and international terrorism, foreign counterintelligence, cybercrime, public corruption, civil rights, organized crime/drugs, white-collar crime, violent crimes and major offenders, and applicant matters. The FBI's investigative philosophy emphasizes close relations and information sharing with other federal, state, local, and international law enforcement, and intelligence agencies. A significant number of FBI investigations are conducted in concert with other law enforcement agencies or as part of joint task forces.
- The FBI's activities are closely and regularly scrutinized by a variety of entities, including Congress, the U.S. Department of Justice, and the Director of National Intelligence.
- The Critical Incident Response Group provides expert assistance in cases involving the abduction or mysterious disappearance of children, crisis management, hostage negotiation, criminal investigative analysis, and special weapons and tactics.

Crisis Messaging Strategy

When a crisis, no matter its nature, has unraveled in any capacity, it is the main goal of the Crisis Incident Response Group to provide accurate and timely information to the media, employees, stakeholders, and the public. It is important to maintain the same messaging strategy across different platforms. Ensure the message strategy is consistent across groups. Ensure all employees in each sector are aware of the messaging strategy and the importance of maintaining it. Depending on the type of crisis, employees of the Federal Bureau of Investigation need to be notified before any public notification related to the crisis.

Press releases will be released solely by the Communications staff of the Critical Incident Response. These will be approved by the Communications Manager, the Public Affairs Specialist, and ultimately the Director of the FBI, who will, in certain situations, express the message to the public.

News releases will be posted to the FBI website <https://www.fbi.gov>. More information will be added as it is obtained and processed to provide more in-depth information to the public.

Key Messages Applicable to Most Crises

1. The FBI's primary focus is to protect the American public, and we are taking all the necessary steps to uphold this commitment.
2. Our hearts go out to all the victims, their families, and all who may have been affected by this crisis.
3. Soon after the incident occurred, the FBI launched an investigation to uncover what happened, identify who was involved, and prevent further harm.
4. We will provide an update as soon as we can do so without threatening the integrity of the investigation or victims.
5. We are asking the public to report any suspicious behavior to the FBI's electronic tip line. For emergencies and life-threatening situations, call 911.

Key Messages

The messaging depends on the crisis, but the key message should always stay the same in each strategy. In times of crisis, the FBI needs to convey a calm and strategic message to the public, especially in times of public panic. The FBI needs to be strategic and understanding in times of crisis. It is of utmost importance to show the public that you are doing everything you can.

Reference page 63 for a key messages template.

Sample messages depending on the type of crisis are listed below.

1. Terrorism/ Counterintelligence

“The FBI is working diligently to provide more information on the recent events that have taken place. We want to state that all governmental agencies are still open and running as before, all with the same mission in mind: to keep the American people safe”.

2. Active Shooter Events/ Hostage Situations/ Kidnappings / Missing Persons

“As this is an ongoing event, there is not much information we can provide at this time. WE would like to remind the American public that the FBI is working tirelessly to address this situation. Our hearts are with all involved”.

3. Cyberattacks

“The FBI is working closely with local authorities. This is an isolated incident, and we want to reassure the public that their personal information is safe and secure.”

4. Reputational Crisis

“The leadership of the FBI is constantly changing and evolving, but our mission does not change. We are committed more than ever in keeping the American people safe and to abide by the Constitution. This mission will never change.”

Key Audiences

Tier 1: The American Public

The key audience will always be the **American Public**. The message is always relayed and curated for them. The FBI works to protect the American people, and this is its main mission. They are built and unified to help governmental entities maintain democratic unity. The message in times of crisis is always curated to help maintain peace and provide comfort in times of crisis.

The American Public is anyone within the entity of the United States that is legally under the jurisdiction of democratic protection. This includes the protection of constitutional rights and freedoms.

Tier 2: Governmental Entities

Another key audience will also be other governmental entities that are either directly or somehow involved in the crisis. These governmental entities can be the White House, the Department of Justice, and local authorities in the city where the crisis occurred. These entities need to be informed secondarily, depending on the crisis. These entities will, at times, be of assistance of the FBI and will need to be informed to be aware of the help that is needed.

Authorized Spokesperson

E. Wade

Public Affair Specialist

Washington, District of Colombia



Communications Platforms

The usage of social media is extremely important during a crisis. In recent years, social media has become the main communication platform to address social, political, and emotional issues to a wide variety of the public. In times of crisis, it is crucial to address the situation using a highly accessible platform to the public, like social media.

The FBI has main lead accounts on all major social media platforms. Utilize these to your advantage. Be aware of social media's limitations and strengths. Keep the message the same throughout each social media platform.

Messaging in communication platforms should remain the same. If there is a loss of life, you first express condolences. If there are any situations where American lives are in danger, appeal to emotion and show you care. The American public wants to hear what you are doing to protect them, not other information.

The use of news outlets is also important; by implementing the same overall strategies through social media and news outlets, you can limit the amount of speculation and rumors about the crisis. Important to strategically invite those outlets that will address the American Public in a way that is not bashing or abrupt but will allow the main message to flow through their broadcast.

Communication is key during a crisis. The public wants you to communicate with them and to inform them of what is going on. They need to be informed to the best of your ability, and it is important to use these communication platforms to your advantage.

Potential Media Questions:

About the Incident

- What can you tell us about the incident?
- How many people have been injured or killed?
- Is there a current threat to the public?
- When did the FBI respond to the incident?
- What FBI units are responding to the incident?
- What is the status of the incident?
- What evidence has the FBI confirmed thus far?
- How long will the investigation be ongoing?

Suspect-Related Questions

- Is there a suspect in custody?
- Do you have a motive for the suspect?
- Did the suspect act alone, or are there other individuals involved?
- Is this an act of terrorism?
- What can you tell us about the suspect?
- Is the suspect tied to any extremist groups?
- Do you believe the suspect committed an act of political violence?

Public Safety Questions

- Is the public in danger?
- What is the FBI doing to protect the public currently?
- Will there be increased safety precautions throughout the ongoing investigation?
- Where should the public report any tips?
- When will we receive an update on the investigation?
- What resources have been made available to victims and their families?
- How will this incident impact future safety precautions?

Media Do's and Don'ts Guidelines

Media Do's

- Respond quickly.
- Stick to verified facts.
- Use the right words.
- Express empathy. Address public concern.
- Address your condolences to the victims, families, and all affected.
- Keep a consistent messaging.
- Focus on informing the audience. Use common language.
- Expect everything you say to appear in print and the electronic media.
- Be strategic with messaging, especially in cases of loss of life.

Media Don'ts

- Don't release unverified or sensitive information.
- Don't use no comment, instead explain why you can't answer.
- Don't harm. Words have consequences.
- Don't disclose victim or personnel identities.
- Don't use "off the record" remarks.
- Don't babble. Know what to say, say it, repeat it.
- Don't lie.
- Don't get defensive or emotional.
- Don't speculate, guess, or assume.
- Don't argue or take offense to comments from the public that you don't agree with.

Social Media Plan

Social media is a useful and effective communication tool that should be used not to distort or complicate messaging but to elevate the main message. Many forms of social media require different messaging strategies.

Posting on social media.

During a crisis in need of FBI assistance, the primary role of monitoring and managing social media falls to the parts of the Critical Incident Response Group. Members of this group will be designated certain tasks that will allow a thorough and detailed overview of information processed and sent to the public in times of heightened crisis.

Primary:

FBI Personal Application Platforms (depending on the situation, information can be expressed quickly to the public)

1. myFBI Dashboard App

Information is released on the application in a quick, urgent manner for the users to see and process.

2. FBI Wanted App

Information, in cases where suspect identification is addressed to the public. This application is also useful in cases of missing persons reports. This is used only when public identification and knowledge of suspects or missing persons in ongoing cases is needed.

Primary Social Media Usage

X (formerly known as Twitter)

3.9M followers

Username: @FBI

1. 280-character limit
2. Useful for a limited, quick, and coordinated response
3. Message from the organization, as unbiased and coordinated as possible.

Director username: FBI Director Kash Patel

- 280-character limit
- Useful for a leadership approach to messaging
- Second to the FBI main account

Example of a limited, quick, and coordinated response

The FBI continues to investigate this afternoon's shooting of two National Guard members in Washington, D.C. If you have any information, please call 1-800-CALL-FBI or visit <http://tips.fbi.gov>.

Instagram:

Used more for non-urgent reminders to the public. It can still be used to address issues or to release important information in different ways to a wider public.

Username: **@FBI**

1K posts & 1.9M followers

Parts of Instagram

1. Carousel posts (multiple pictures in one singular post)
 - It can be used to address multiple parts of an ongoing investigation.
 - Also provides the public with more physical evidence.
2. Instagram stories
 - 24-hour time frame
 - Important for a quick and urgent response

YouTube:

Used in video format to inform the public. It is useful in certain cases where in-depth discussion and information are vital to the investigation.

Username: FBI-Federal Bureau of Investigation

285K Subscribers & 1.1K videos

- Ability to produce longer videos to release more information.
- Common place to post press releases & public conference.

Social Media Advantages

- Provides immediate information to a wide public audience.
- Can reach a wider public audience using multiple different outreach platforms.
- Beneficial in situations where structured rumors take hold of a certain crisis and provide factual and immediate information to calm the public.
- Helps to create meaningful relationships with the public.
- Used to gauge public emotions about certain topics and likely crises.

Social Media Disadvantages

- Social media can, at times, heighten public concern to extremes.
- Information that can be limited
- Allows the public to input their personal biases, which can affect public concern.
- Social media can be time-consuming and must be constantly monitored for rumors and heightened public disarray.
- Certain publics involved in certain crises can be hard to inform without social media.

Tips for Social Media Messaging:

- Important to be accurate and concise.
- Important (if directly involved in a crisis) to be first to get ahead of the story.
- Important to be consistent in messaging.
- Identify who is providing the information (FBI Director, Critical Incident Response Group, Police Department, White House)
- Follow guidelines specific to the social media platform.
- Provide links to the main website whenever possible.
- Correct misinformation in an efficient way that disregards argumentative tones.
- Monitor responses to your messaging on other platforms
- Be strategic on other posts of other incidents while the crisis is underway.

EXAMPLES



Office of Public Affairs

950 Pennsylvania Ave.
Washington, D.C. 20530

FOR IMMEDIATE RELEASE:

Dec. 2, 2025

CONTACT:

Office of Public Affairs
202-278-3519

MEDIA ADVISORY**FBI AND ICE TO COVER RECENT ENFORCEMENT INCIDENTS ACROSS THE U.S.**

WHAT: The Federal Bureau of Investigation (FBI) and Critical Incident Response Group (CIRG) are issuing an update regarding concerns of ICE and FBI agent impersonations, and broader concerns about public safety.

WHO: Federal Bureau of Investigation Critical Incident Response Group
United States Immigration and Customs Enforcement Public Affairs Team

WHEN: Tuesday, Dec. 2, 2025
10 a.m.

Scheduled activities:

9:30 a.m. Cameras and the media set up.

9:50 a.m. Reporters show up to location.

10 a.m. Introductory statement by CIRG Assistant Director, Devin Kowalski.

10:10 a.m. Media Q&A.

WHERE: FBI Headquarters, J. Edgar Hoover Building, Washington, D.C.

###

Office of Public Affairs

950 Pennsylvania Ave.
Washington, D.C. 20530

FOR IMMEDIATE RELEASE:

Dec. 2, 2025

CONTACT:

Office of Public Affairs
202-278-3519

FBI AND ICE COVERS RECENT ENFORCEMENT INCIDENTS ACROSS THE U.S.

WASHINGTON, D.C. — The Federal Bureau of Investigation, in coordination with the U.S. Immigration and Customs Enforcement, issued a joint statement regarding heightened public concern surrounding several law enforcement incidents across the United States. Over the past few weeks, both organizations have worked collaboratively to ensure all non-U.S. citizens who have engaged in criminal activity are identified and apprehended in accordance with federal immigration laws.

“The FBI remains committed to protecting the American public, while maintaining our standards of transparency, accountability, and integrity,” said FBI Director Kash Patel. “We continue to uphold federal law every day, and our interagency collaboration with ICE enhances our ability to protect communities across the U.S.”

Both agencies acknowledge the questions and concerns that have emerged in response to recent enforcement incidents across the U.S. The FBI and ICE are reviewing all reported incidents to ensure all operations are carried out constitutionally and professionally.

“Maintaining public trust is one of our utmost commitments”, said both the FBI and ICE. “Our work will always be guided by the Constitution and federal law. We will not compromise public safety or the rights of individuals when carrying out federal immigration enforcement.

About the Federal Bureau of Investigation

The FBI is an intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities. It is the principal investigative arm of the U.S. Department of Justice and a full member of the U.S. Intelligence Community. The FBI has the authority and responsibility to investigate specific crimes assigned to it and to provide other law enforcement agencies with cooperative services, such as fingerprint identification, laboratory examinations, and training. The FBI also gathers, shares, and analyzes intelligence, both to support its own investigations and those of its partners and to better understand and combat the security threats facing the United States.

Office of Public Affairs

950 Pennsylvania Ave.
Washington, D.C. 20530

FOR IMMEDIATE RELEASE:

Dec. 2, 2025

CONTACT:

Office of Public Affairs
202-278-3519

MEDIA ADVISORY**FBI OFFICIALS TO BRIEF NATION ON TARGETED ATTACK
AGAINST NATIONAL GUARD PERSONNEL**

WHAT: The Federal Bureau of Investigation (FBI) will provide a national briefing regarding the recent attack on the National Guardsmen with high-level information on the incident and suspect.

WHO: Kash Patel, FBI Director
Jeanine Pirrio, United States Attorney for the District of Columbia

WHEN: Thursday, Nov. 27, 2025
9:15 a.m.

Scheduled activities:

9:16 a.m. Opening statement by Jeanine Pirrio.

9:23 a.m. Kash Patel speaks on the incident.

WHERE: FBI Headquarters, J. Edgar Hoover Building, Washington, D.C.

###

Office of Public Affairs

950 Pennsylvania Ave.
Washington, D.C. 20530

FOR IMMEDIATE RELEASE:

Dec. 2, 2025

CONTACT:

Office of Public Affairs
202-278-3519

FBI BRIEFS NATION FOLLOWING DEADLY ATTACK ON NATIONAL GUARD PERSONNEL

WASHINGTON, D.C. — The Federal Bureau of Investigation today released new details on the attack in Washington, D.C., where two National Guard members were attacked on Wednesday evening. Officials have a suspect in custody, and charges have now been made.

“Our condolences go out to the victim’s families during this time,” said FBI Director Kash Patel. “We are reviewing and reinforcing security measures to ensure our nation is protected, as safety is one of our top priorities.”

The Trump Administration has addressed the attack as targeted. The two victims, Sarah Beckstrom and Andrew Wolfe, were targeted near the corner of 17th and I Street, where the suspect came around the corner firing. Beckstrom died Thursday evening, while Mr. Wolfe remains in critical condition.

Jeanine Pirrio, U.S. Attorney for the District of Columbia, said, “We are doing everything to assist the family and make sure they are well taken care of during this difficult time.”

The suspect, Rahmanullah Lakanwal, has been charged with assault to murder in the first degree as well as three counts of assault with the intent to kill while armed and criminal possession of a weapon. New details on the suspect say he came to the U.S. from Afghanistan in 2021, where he had a relationship with the CIA.

“This is an ongoing process as we investigate more about the suspect and his background,” said Patel. “We will not stop until we find a reason behind this targeted attack. We have multiple strong forces investigating this case, and I strongly believe we will crack this down.”

-MORE-

About the Federal Bureau of Investigation

The FBI is an intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities. It is the principal investigative arm of the U.S. Department of Justice and a full member of the U.S. Intelligence Community. The FBI has the authority and responsibility to investigate specific crimes assigned to it and to provide other law enforcement agencies with cooperative services, such as fingerprint identification, laboratory examinations, and training. The FBI also gathers, shares, and analyzes intelligence, both to support its own investigations and those of its partners and to better understand and combat the security threats facing the United States.

Office of Public Affairs

950 Pennsylvania Ave.
Washington, D.C. 20530

FOR IMMEDIATE RELEASE:

Dec. 2, 2025

CONTACT:

Office of Public Affairs
202-278-3519

MEDIA ADVISORY**FEDERAL BUREAU OF INVESTIGATION TO PROVIDE UPDATE ON
CYBERSECURITY CRIMINALS DURING HOLIDAYS**

WHAT: The Federal Bureau of Investigation (FBI), in coordination with the Cyber Division Group, is addressing the recent cyberattacks and financial scams during the busiest online shopping time of the year

WHO: Federal Bureau of Investigation Cyber Division Group

WHEN: Tuesday, Dec. 2, 2025
10 a.m.

Scheduled activities:

9:30 a.m. Cameras and the media set up.

9:50 a.m. Reporters show up to the location.

10 a.m. Introductory statement by Cyber Division Assistant Director, Brett Leatherman.

10:10 a.m. Media Q&A.

WHERE: FBI Headquarters, J. Edgar Hoover Building, Washington, D.C.

###

Office of Public Affairs

950 Pennsylvania Ave.
Washington, D.C. 20530

FOR IMMEDIATE RELEASE:

Dec. 2, 2025

CONTACT:

Office of Public Affairs
202-278-3519

**FBI PROVIDES UPDATES ON CYBERSECURITY AS
SHOPPING HEIGHTENS DURING THE HOLIDAY SEASON**

WASHINGTON, D.C. — The FBI is warning consumers to be on high alert during this holiday season. There are many types of online scams that criminals use to strip one of their hard-earned money or personal information this holiday season.

It is important to take time to do your research before giving your money away. If a deal seems too good to be true, it probably is. Cybersecurity threats can range from online shopping websites to fake charity organizations seeking donations. The FBI strongly advises the American public to proceed with caution and take the time to verify all information before inputting personal information.

“The FBI receives thousands of reports every year of people being scammed during the holidays, and last year alone, the American public lost over 600 million dollars to online scammers,” said the Director of the FBI. “Do not let scammers rob you of your joy this holiday season. Stay smart and aware of suspicious online activity.”

The most common scams we are seeing affecting the public is non-delivery scams, where one pays for the goods, but they are never delivered, gift card fraud, where websites or emails give away “free” gift cards, or fake charities, where scammers impersonate well-known and trusted organizations to solicit donations through phone calls, emails, and social media to steal funds.

“To protect yourself this holiday season, here are a few tips. Don’t click on any suspicious links or attachments in emails, on websites, or through social media,” said the Director of the FBI. “Check each website’s URL to make sure it’s legitimate and be wary if a company asks you to update your password or account information. Lastly, if you ordered a package online, always get a tracking number for your purchase.”

-MORE-

CYBER ATTACKS / PAGE 2 OF 2

The FBI is committed to keeping our communities safe, in person and online. We encourage everyone to take the time to review online purchases and charitable donations. If you happen to fall victim to a holiday scam or charity fraud, the FBI urges you to submit a complaint to the FBI's Internet Crime Complaint Center at ic3.gov as soon as possible, report it to your local law enforcement, and contact your credit card company immediately to stop, reverse, or dispute any suspicious charges.

Stay Safe this holiday season. Remember to always do your research.

About the Federal Bureau of Investigation

The FBI is an intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities. It is the principal investigative arm of the U.S. Department of Justice and a full member of the U.S. Intelligence Community. The FBI has the authority and responsibility to investigate specific crimes assigned to it and to provide other law enforcement agencies with cooperative services, such as fingerprint identification, laboratory examinations, and training. The FBI also gathers, shares, and analyzes intelligence, both to support its own investigations and those of its partners and to better understand and combat the security threats facing the United States.

Holding Statement

The FBI warns of cyber criminals impersonating financial institutions to steal money or information in Account Takeover (ATO) fraud schemes. The cyber criminals target individuals, businesses, and organizations of varied sizes and across sectors. In ATO fraud, cyber criminals gain unauthorized access to the targeted online financial institution, payroll, or health savings account, to steal money or information for personal gain. Since January 2025, the FBI Internet Crime Complaint Center (IC3) has received more than 5,100 complaints reporting ATO fraud, with losses exceeding \$262 million.

HOW IT WORKS

The cybercriminal impersonates the financial institution's staff or website to obtain access to the account. Cyber criminals usually gain access to accounts through social engineering techniques — including texts, calls, and emails — or through fraudulent websites.

Social Engineering

- A cybercriminal manipulates the account owner into giving away their login credentials, including multi-factor authentication (MFA) code or One-Time Passcode (OTP), by impersonating a financial institution employee, customer support, or technical support personnel. The cybercriminal then uses login credentials to log into the legitimate financial institution website and initiate a password reset, ultimately gaining full control of the accounts.
- Social engineering methods include contacting account owners via fraudulent text messages, calls, or emails to trick the email recipient into providing their login credentials. In some instances, the cybercriminal states that there are fraudulent transactions on the financial account and may provide a link to a phishing website that the account owner believes will report the fraud or prevent additional fraudulent transactions.
- In some instances, cyber criminals impersonating financial institutions reported to the account owner that their information was used to make fraudulent purchases, including firearms. The cybercriminal convinces the account owner to provide information to a second cybercriminal impersonating law enforcement, who then convinces the account owner to provide account information.

Phishing Domains/Websites

- The cybercriminal uses a phishing website that looks like a legitimate online financial institution or payroll website to trick the account owner into giving away their login credentials. Believing the phishing website is the legitimate one, users enter their login credentials into the fraudulent site, unknowingly providing them to cyber criminals.
- Cyber criminals may also use a technique called Search Engine Optimization (SEO) poisoning. *SEO poisoning* refers to cyber criminals purchasing ads that imitate legitimate

business ads to increase the prominence of their phishing websites by making them appear more authentic to customers who use a search engine to locate the business's website. When users click on the fraudulent search engine ad, they are directed to a sophisticated fraudulent phishing site that mimics the real website, tricking users into providing their login information.

Once the impersonators have access and control of the accounts, the cyber criminals quickly wire funds to other criminal-controlled accounts, many of which are linked to cryptocurrency wallets; therefore, funds are disbursed quickly and are difficult to trace and recover. In some cases, including nearly all social engineering cases, the cyber criminals change the online account password, locking the owner out of their own financial account(s).

STAY PROTECTED

Stay vigilant against ATO fraud attempts by following these tips.

- Be careful about the information you share online or on social media.
- By openly sharing information like a pet's name, schools you have attended, your date of birth, or information about your family members, you may give scammers the information they need to guess your password or answer your security questions.
- Monitor your financial accounts on a regular basis.
- Watch for irregularities, such as missing deposits or unauthorized withdrawals, wire transfers, or expenditures.
- Always use unique, complex passwords.
- Enable two-factor authentication or MFA on any account possible. Never disable it.
- Use Bookmarks or Favorites for navigating to login websites.
- Avoid clicking on Internet search results or advertisements. MFA will not protect you if you land on a fraudulent login page. Carefully examine any email address, URL, or spelling in unsolicited correspondence.
- Stay vigilant against phishing attempts.
- Be suspicious of unknown "banking" or "company" employees who call you; don't trust the caller ID. Hang up, verify the correct number, and call it yourself. Companies generally do not contact you to ask for your username, password, or OTP.

WHAT TO DO IN CASE OF AN ATO INCIDENT

1. Contact Your Financial Institution

Contact your financial institution as soon as fraud is recognized to request a recall or reversal, as well as a Hold Harmless Letter or Letter of Indemnity. Requesting a recall and obtaining a Hold Harmless Letter/indemnification document as quickly as possible may reduce or eliminate your financial losses. Immediately report fraudulent wire transfers to both your financial institution and to the FBI Internet Crime Complaint Center (IC3) at www.ic3.gov.

2. Reset or Revoke Compromised Credentials

Reset all credentials and passwords that may have been exposed during the intrusion, including user and service accounts, compromised certificates, or other "secret" credentials. If you use the compromised password for other online accounts, change your password on those sites too.

3. File a Complaint

File a detailed complaint with www.ic3.gov. The complaint must contain all required data in the provided fields, including banking information.

- Identifying information about the cyber criminals, including the financial institution impersonated, name, phone number, address, and email address.
- Any websites or software that the cyber criminals may have asked you to visit or download.
- Any financial accounts provided or used by the cyber criminals.
- Include the words "Account Takeover" or "SEO poisoning" in the incident description.

4. Notify the Impersonated Company

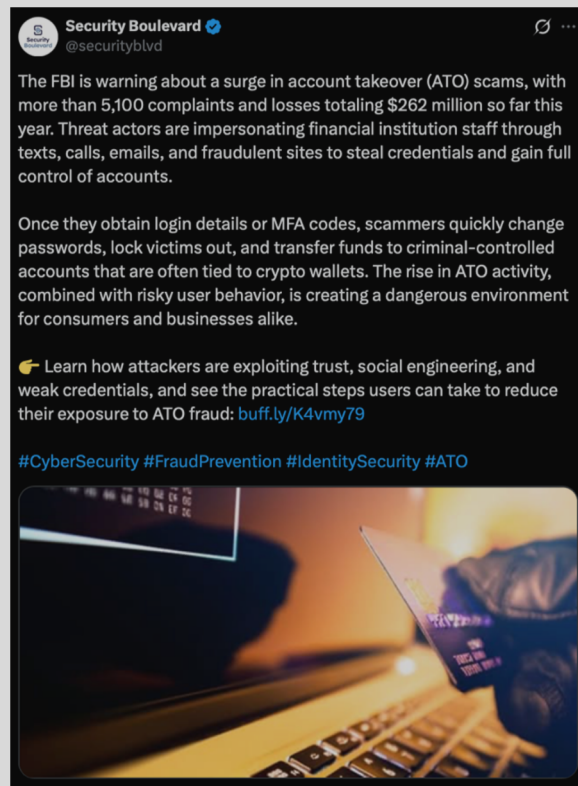
Notify the company that was impersonated of the method the cyber criminals used to target the account owner. The company may be able to warn others to watch out for the scam and take proactive measures, like requesting that phishing pages be taken down.

5. Stay Informed

Visit www.ic3.gov for updated Industry Alerts and Public Service Announcements regarding ATO trends, as well as other cyber-enabled fraud schemes.

Social Media Posts

“X” Posts



Instagram



News Source



Media Kit



Office of Public Affairs

950 Pennsylvania Ave.
Washington, D.C. 20530

FOR IMMEDIATE RELEASE:

Nov. 10, 2025
{insert date}

CONTACT:

Office of Public Affairs
202-278-3519

MEDIA ADVISORY
**FBI TO ADDRESS AGENCY OVERSIGHT
AND OPERATIONAL CONCERNS**

WHAT: The Federal Bureau of Investigation (FBI) and Critical Incident Response Group are issuing the ongoing interagency collaboration, along with leadership and organizational challenges amid review of high-profile investigations.

WHO: Federal Bureau of Investigation Critical Incident Response Group

WHEN: Friday, Nov. 14, 2025
10 a.m.

Scheduled activities:

9:30 a.m. Reporters and journalists arrive.

10 a.m. Introduction statement by Valerie Fields.

WHERE: 305 Carroll Hall (Freedom Forum Conference Room)

NOTE: If unable to attend in person, there will be a remote option via Zoom for those who are out of town or prefer a virtual option. Please [click the Zoom link](#) to register and confirm your attendance.

###

Office of Public Affairs
950 Pennsylvania Ave.
Washington, D.C. 20530

FOR IMMEDIATE RELEASE:
Nov. 10, 2025

CONTACT:
Office of Public Affairs
202-278-3519

**FBI ADDRESSES PUBLIC QUESTIONS ON LEADERSHIP,
ICE COLLABORATION, AND THE EPSTEIN FILES**

WASHINGTON, D.C. — Today, the Federal Bureau of Investigation addressed the public's questions surrounding the agency's leadership, interagency collaboration with the U.S. Immigration and Customs Enforcement Agency, and the Epstein Files.

"Regardless of changes within our organization, the FBI remains committed to its mission to protect the American people and to ensure that every investigation upholds the highest integrity of the law," said the FBI's Critical Incident Response Group.

In January 2025, the President of the United States appointed a new director for the FBI. Since assuming this role, Director Kash Patel has worked to guide the FBI through organizational transition. The FBI director leads the FBI's day-to-day operations, overseeing all aspects of the bureau's functions, which include national security, intelligence, and criminal investigations.

"I am proud of the work of the FBI," said Patel. "As we move forward, our mission remains the same: to ensure the American people are protected and justice is brought forth in a fair and transparent process."

The FBI and ICE are federal law enforcement agencies. The FBI operates under the Department of Justice, and ICE operates under the Department of Homeland Security. While the FBI and ICE are two separate agencies, they have recently worked in compliance with one another to enforce federal immigration laws put in place by the current White House administration.

"Interagency collaboration is essential to upholding federal law," said an FBI spokesperson. "We are aware of how emotionally charged this issue is, but our collaboration with ICE remains focused on ensuring that operations occur within compliance with federal law."

-MORE-

FBI / PAGE 2 OF 2

As of today, the FBI has publicly released over 43,000 documents related to the investigation of Jeffrey Epstein. The FBI is a law enforcement agency that continues to review and confirm evidence to ensure the accuracy of all information released to the public. Confirmed evidence is presented to the Department of Justice for a decision on prosecution, and depending on the outcome of an investigation, evidence is either returned or retained for court.

“As this is an ongoing investigation, the FBI is committed as ever to bring justice to the victims of this crime and to maintain protection in a fair and transparent process,” said the CIRG.

About the Federal Bureau of Investigation

The FBI is an intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities. It is the principal investigative arm of the U.S. Department of Justice and a full member of the U.S. Intelligence Community. The FBI has the authority and responsibility to investigate specific crimes assigned to it and to provide other law enforcement agencies with cooperative services, such as fingerprint identification, laboratory examinations, and training. The FBI also gathers, shares, and analyzes intelligence, both to support its own investigations and those of its partners and to better understand and combat the security threats facing the United States.

TEMPLATES



Incident Report

FBI CIRG DIVISION

REPORT ID / INCIDENT NAME: _____

DATE / TIME OF REPORT FILED: _____ (MM/DD/YYYY)
(HH:MM)

DATE / TIME INCIDENT OCCURRED: _____ (MM/DD/YYYY)
(HH:MM)

LOCATION(S) OF INCIDENT: _____

INCIDENT DESCRIPTION: _____

CIRG UNIT / BRANCH RESPONDING: _____

REPORTING OFFICER / AGENT NAME _____

POINT OF CONTACT (phone, email, other): _____

OTHER AGENCIES / PARTNERS INVOLVED: _____

Incident Type (check one or more):

- ☐ Hostage / Barricade / Siege
- ☐ Active Shooter / Violent Crime / Armed Offender
- ☐ Bomb Threat / Explosive Device / Hazardous Device Incident
- ☐ Child Abduction / Missing Child / Kidnap
- ☐ Terrorism / WMD / CBRN Threat
- ☐ Natural Disaster / Mass Casualty / Major Crash (air, train, etc.)
- ☐ Prison Riot / Mass Disturbance / Public Safety Threat
- ☐ Other: _____

Detailed Description of Incident (what happened / observed / reported):

Copies To: Devin J. Kowalski / Assistant Director, Critical Incident Response Group

Media Inquiry Log

CONTACT PERSON:

CONTACT'S POSITION/TITLE:

CONTACT'S E-MAIL ADDRESS:

CONTACT'S TELEPHONE NUMBER:

CONTACT'S ORGANIZATION/COMPANY/AFFILIATION:

PROJECT: ☐ PODCAST ☐ BOOK ☐ MAGAZINE

☐ FILM/MOTION PICTURE ☐ TELEVISION

PLEASE DESCRIBE WHAT YOU ARE LOOKING FOR FROM THE FBI:

FBI CIRG – Post-Crisis Evaluation Form

Incident Name / ID: _____

Date/Time of Incident: _____

Location: _____

Evaluator Name / Position / Unit: _____

Role in the Incident: ☐ Field Respondent ☐ Supervisor ☐ PIO / Public Affairs ☐ Other:

1. Notification & Communication Effectiveness

Question	Rating	Comments / Suggestions
Timeliness of incident notifications	☐ Excellent ☐ Good ☐ Fair ☐ Poor	
Clarity and completeness of notifications	☐ Excellent ☐ Good ☐ Fair ☐ Poor	
Suggestions for improving notification processes		

2. Operational Performance Feedback

Question	Rating	Comments / Suggestions
Overall effectiveness of CIRG response	☐ Excellent ☐ Good ☐ Fair ☐ Poor	
Key strengths of the response:		
Areas needing improvement:		

3. Crisis Communication & Media Handling (if applicable)

Question	Rating	Comments / Suggestions
Coordination with Public Affairs Officer (PIO)	☐ Excellent ☐ Good ☐ Fair ☐ Poor	
Handling of media inquiries and public communications	☐ Excellent ☐ Good ☐ Fair ☐ Poor	
Suggestions for improving media communications		

4. Crisis Communication Plan (CCP) Feedback

Question	Rating	Comments / Suggestions
Effectiveness of the CCP in guiding actions	☐ Excellent ☐ Good ☐ Fair ☐ Poor	
Suggestions for improving the CCP for future incidents		

5. Overall Feedback

Additional comments or observations:

[illegible]

Key Messages Template

This template should be used to plan out the three key messages a spokesperson should stick to within a press conference related to a crisis. Staying on message is essential to maintain clear and consistent messaging among the public.

Key Message #1

Key Message #2

Key Message #3

Social Media Post Templates

Platform - X

**Federal Bureau of Investigation** 
@FBI

Reset

Insert Text (280 max characters)

 Drag and drop or click here to add image

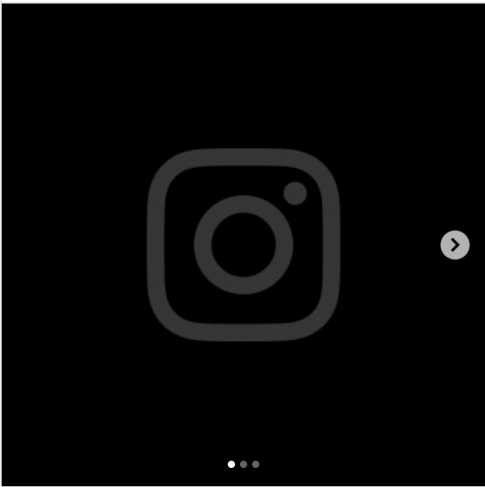
9:09 AM · Sep 02, 2025 · 0 Views

0 Retweets · 0 Quotes · 0 Likes · 0 Bookmarks



Platform - Instagram

**@FBI** · 22s
Washington, D.C.





1,234 likes

@FBI Insert Text

View all 1,234 comments

Media Advisory Template

Office of Public Affairs

950 Pennsylvania Ave.

Washington, D.C. 20530

FOR IMMEDIATE RELEASE:

{insert date}

CONTACT:

Office of Public Affairs

202-278-3519

MEDIA ADVISORY
INSERT TITLE

WHAT: {Insert description of event}**WHO:** Federal Bureau of Investigation Critical Incident Response Group**WHEN:** [Insert date]
[Insert time]

Scheduled activities:

[time] [description]

[time] [description]

WHERE: [insert location]**NOTE:** [insert note]

###

News Release Template

Office of Public Affairs

950 Pennsylvania Ave.
Washington, D.C. 20530

FOR IMMEDIATE RELEASE:

[insert release date]

CONTACT:

Office of Public Affairs
202-278-3519

[INSERT TITLE OF NEWS RELEASE]

[CITY, STATE] — LEAD PARAGRAPH

INSERT BODY

INSERT QUOTE

INSERT BODY

BOILERPLATE**About the Federal Bureau of Investigation**

The FBI is an intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities. It is the principal investigative arm of the U.S. Department of Justice and a full member of the U.S. Intelligence Community. The FBI has the authority and responsibility to investigate specific crimes assigned to it and to provide other law enforcement agencies with cooperative services, such as fingerprint identification, laboratory examinations, and training. The FBI also gathers, shares, and analyzes intelligence, both to support its own investigations and those of its partners and to better understand and combat the security threats facing the United States.